Seccom Flex User manual

1 About the Flex communication service

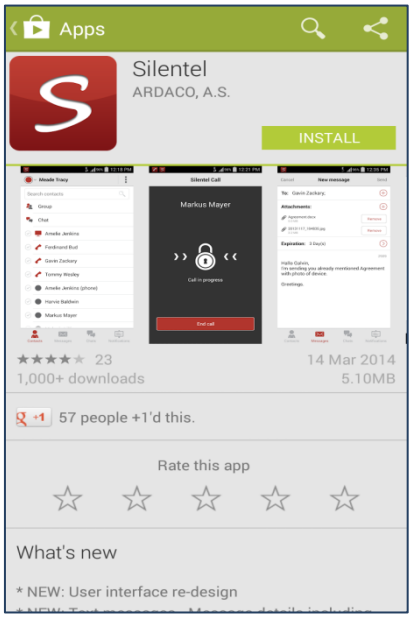
Seccom Flex is an end-to-end secured communication service based on the **NATO-approved** platform **Silentel**. In order to use the **Flex** service, the **Silentel** application must be installed on the user's smartphone, tablet or PC.
The service can be used on iPhone, iPad, most Android phones/tablets, BlackBerry 10.x and Windows XP, Vista, 7 and 8, and includes voice, text messages, e-mail and chat conference (depending on your organizations choice).

Flex is a closed communication service between registered users that can be used for internal communication or between organizations that have implemented the service. Both the sender and recipient must have a **Flex account** and the **Silentel application** installed. The communication is Internet-based and can use on 2/3/4G mobile data connection, Wi-Fi, fixed networks or satellite-based Internet connection.

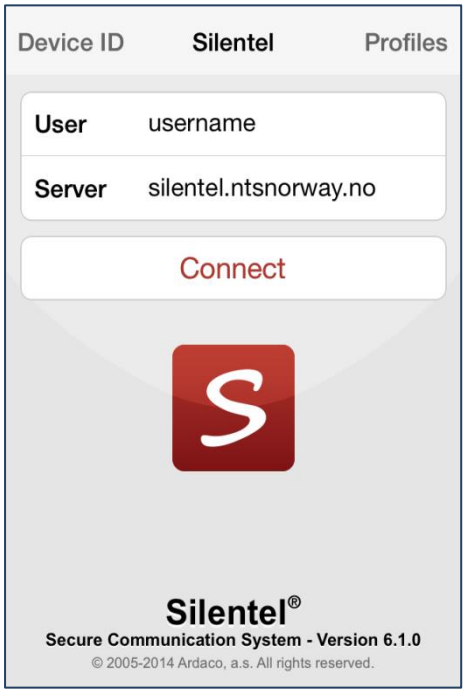
All communication is end-to-end encrypted with AES256 and RSA2048, and meets the requirements on the level of **NATO Restricted**. The solution uses one-time encryption keys established using the Diffie-Hellman-algorithm for each new conversation and text message. There is no technical possibility for other parties than the sender and receiver to access the communication, neither for Seccom, public authorities or other parties.

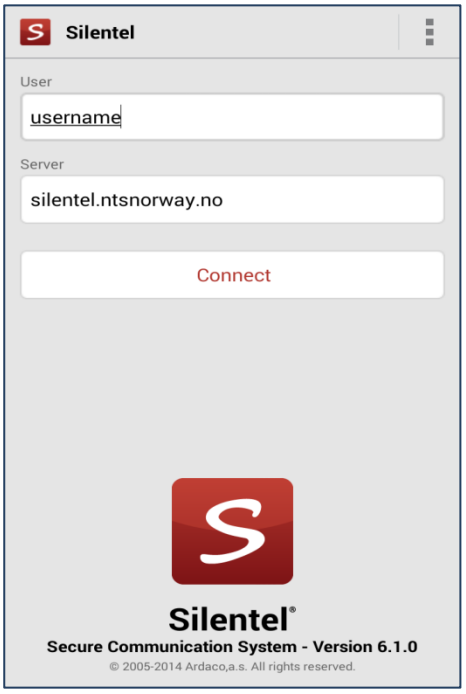
2 Getting started with Flex

1. In order to install **Silentel**, the Android-user needs a Google-account and the iOS-user must have an Apple ID. Everyone having installed applications on the phone will have this.
   See https://play.google.com/ or https://appleid.apple.com/
2. Install **Silentel** on
   -Android telephone or tablet from Google Play
   -iPhone or iPad from App store
   -PC from http://www. silentel.com/support/windows



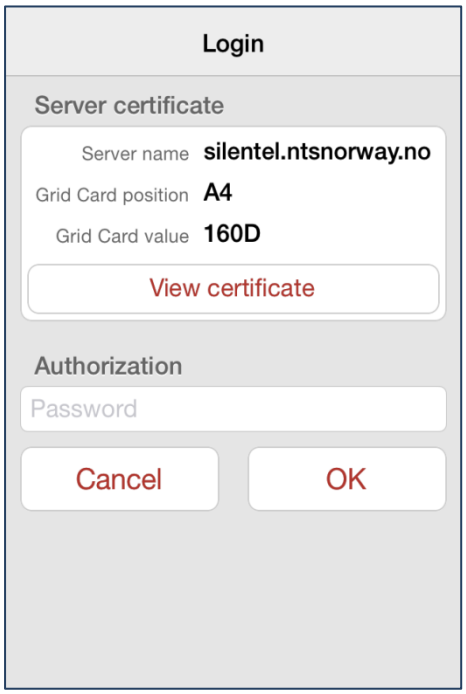
3. Start the application and enter the **Username** and **Silentel server** information received either by e-mail from Seccom or from your organizations **Flex Superuser**:
   Silentel server: **silentel.ntsnorway.no**
   Note! This must be changed in the downloaded application!

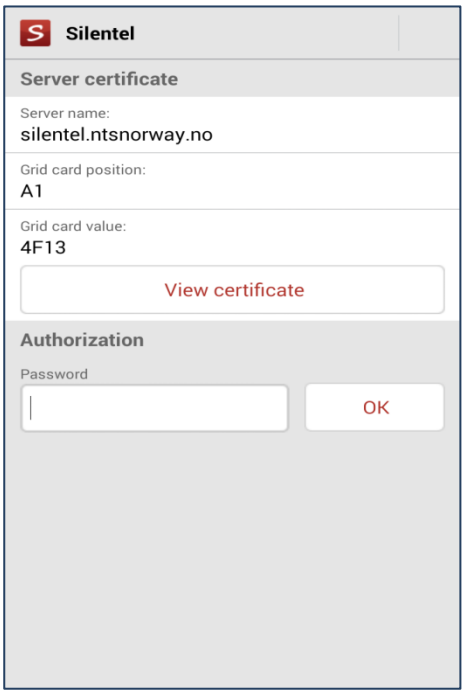




Username and password are the same for all platforms, and can be used alternately, but only on one device at the time.

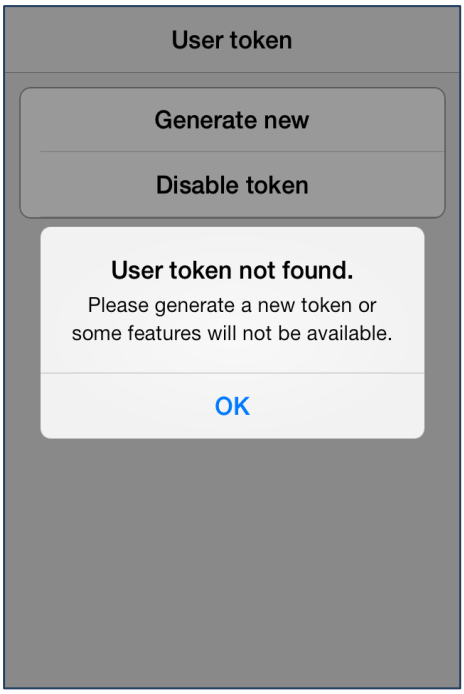
4. Click **Connect,** and the password window is shown.

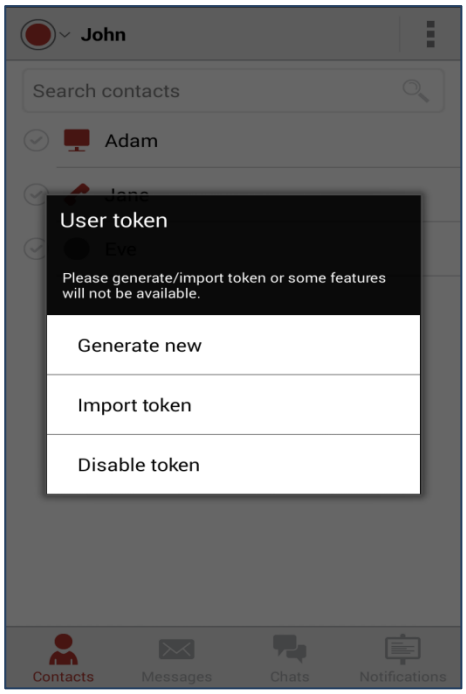




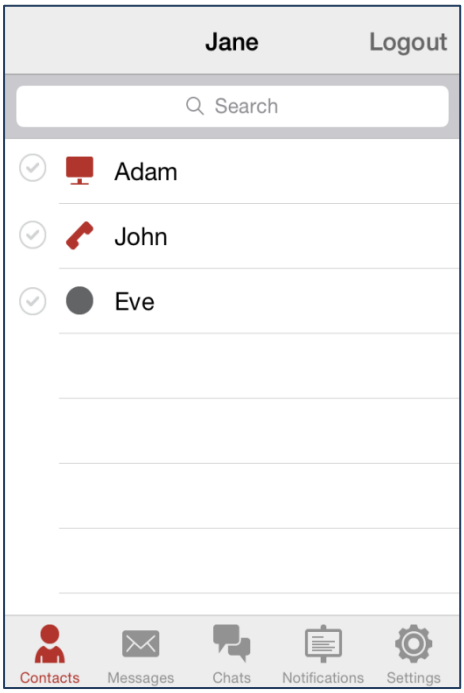
Enter **Password** and click **OK**:

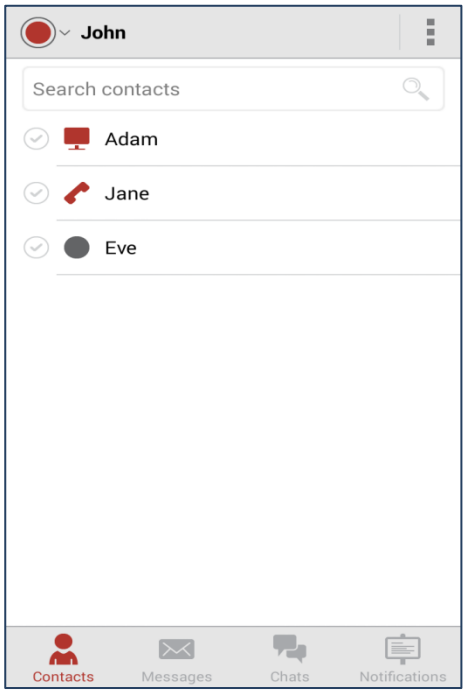
If it is the first time login (or when changing devices) the application will ask to generate **User token** (private encryption key used for text messages and e-mail).
Click **Generate new / Generate.**





5. The main window with the users address list is displayed:



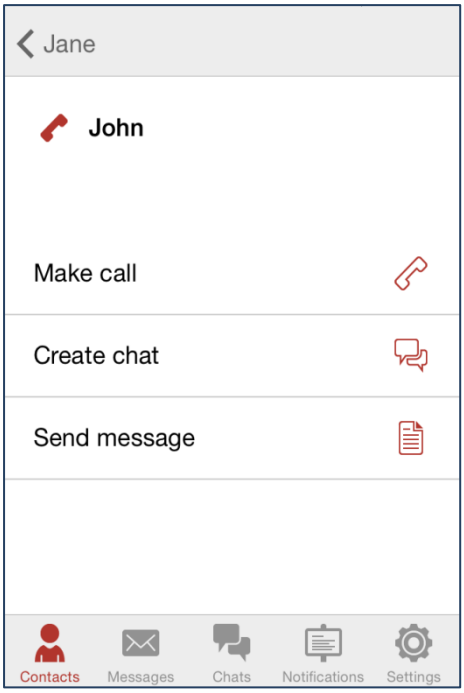


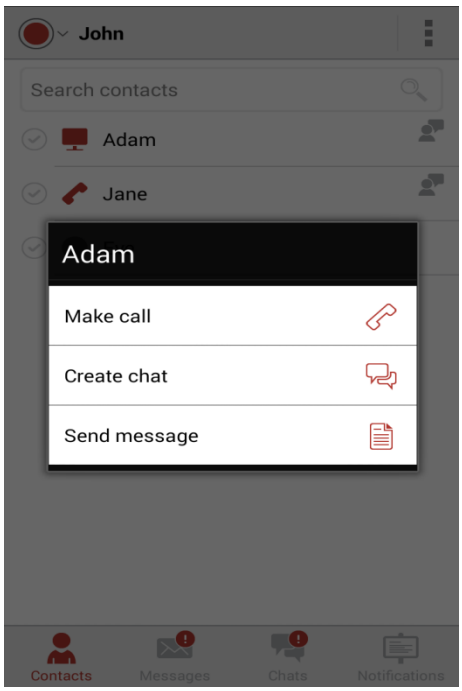
John	User online on mobile/tablet
Adam	User online on PC
Eve	User offline. Not available for voice calls or chats, only messages/mail

3 Flex functions

3.1 Voice calls

To make a **call**, click on a contact and select **Call / Make call**:

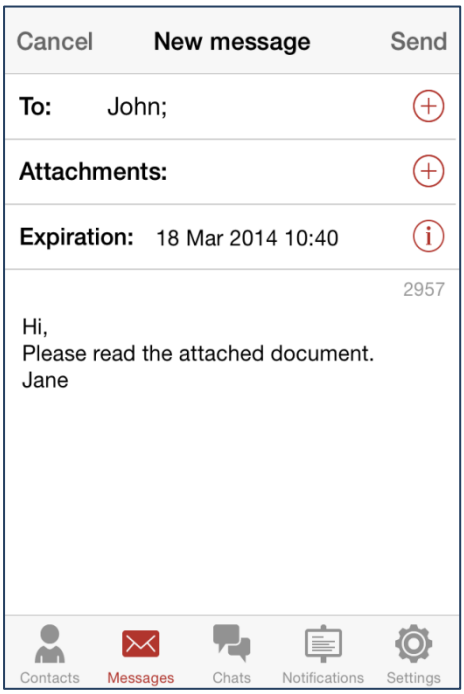


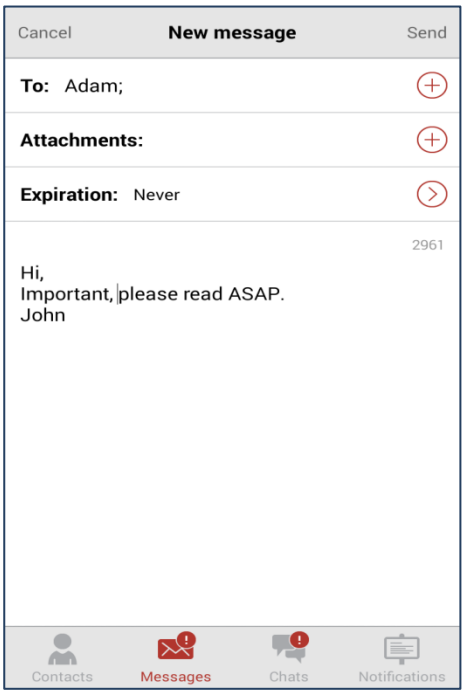


Wait until the notification tone ends and the call is set up. It is only possible to set up and receive calls when the user is online and logged in. **Missed calls** are shown with an alert symbol in the status bar and under **Notifications** in the application.

3.2 Text messages and e-mail

To send a **text message or s-mail**, click on a contact and select **Send message:**





Mail users can attach photos, videos or files (files only on Android, BlackBerry and Windows PC due to limitations in iOS file management system).
Lifespan can be set for text messages/s-mail under **Expiration**. If this is changed from **Never**, the message will be automatically deleted after the given time period regardless if the recipient has read the message or not. If the recipient has not read the message before the time expires, he/she will only receive a notification that a message was received from the sender that has expired.

Text messages and mails are not stored on the mobile device/PC, but encrypted on the **Flex**-server with encryption keys available only to the sender and receiver. This means that access to the mobile device does not give access to stored messages and files if the user is not logged in, and the information stored on the server is not accessible to anyone else than the sender and receiver.

Text messages/s-mail can only be sent when the user is logged in. Messages/s-mail can also be sent to offline users. They can access the messages after logging in.

To send the same message to multiple recipients, all the recipient should be selected in the circle on the left side and then click on one of the selected contacts and choose **Send message**.

3.3 Received messages - Inbox

Received messages are indicated with a symbol in the telephones status bar and in the application.
Go to **Messages** and **Inbox** to read received messages.

The Sender will be able to see that the message is received and read in the **Sent**-folder.

3.4 Sent messages - Sent

Sent messages are stored under **Sent**, and it is possible to see if the recipient has received and read the messages.

A white, closed envelope means that the message is not delivered to the recipient, i.e. the recipient has not been logged in after the message was sent.

A red, closed envelope means that the message is delivered to the recipient, but not read.
A red clock-symbol indicates that automatic deletion with **Lifespan** has been set up.

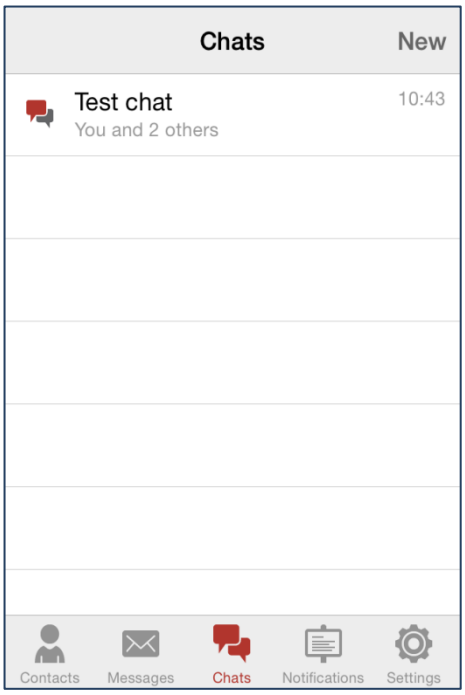
A grey, open envelope shows that the message has been read by the recipient.
A paper clip symbol on the right side indicates that the message has an attachment.

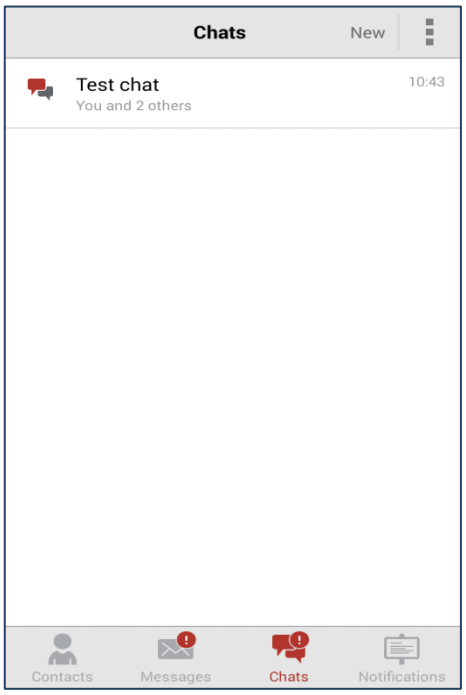
If the message is sent to multiple recipients, a copy of the message will be stored in the **Sent**-folder for each recipient making it possible to track delivery and read status for each recipient individually.

3.5 Chat conference

Multiple simultaneous chat-sessions can be set up with unlimited users in each session. This can be used for group based instant messages and direct file transfer.

Select the participants from the address list and choose **Create chat**. Enter a name for the chat session and click **Create**.

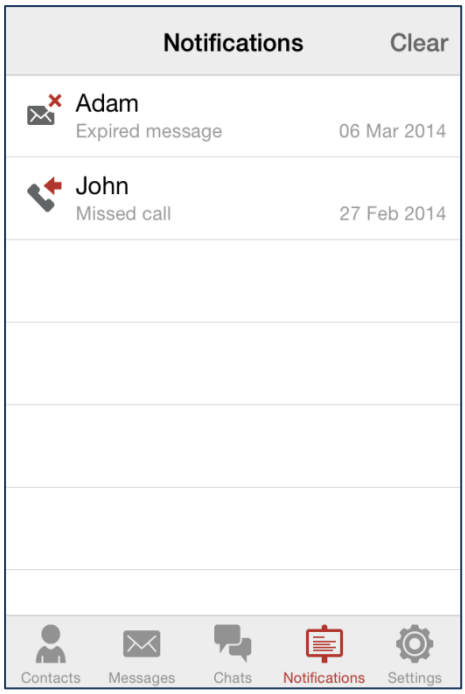




The chat sessions are active until the user manually leaves the session or logs out from the server. To leave a chat session, select **Menu**, **Leave chat** on Android. On iPhone choose **Info** and **Leave**.

3.6 Notifications

Missed calls (both when the user is online and offline) will be shown under **Notifications** together with an overview of messages not read before they were automatically deleted using **Lifespan**.



3.7 Bluetooth and speakerphone function

Speakerphone and Bluetooth for connecting external loudspeaker or handsfree solutions are not supported in standard issue of the **Silentel**-application. It would be against its purpose to use maximum security for the communication channel and at the same time letting the communication be broadcasted at the endpoints.

Bluetooth can broadcast the signal 30 meters and more around the receiving device, and is not sufficiently encrypted to be recommended in connection with using **Silentel**. Special versions of the **Silentel** application are available if a secure Bluetooth solution is to be used.

Using speakerphone opens for capturing both sides of the voice call in case the room is bugged, and should be used with caution. On a computer or tablet speakerphone is supported as this is often the only available solution for this kind of devices.
Tablets are recommended as a replacement for ordinary speakerphones when needed.

3.8 Using Flex Guest account

All **Flex-users** have the possibility to have a **personal guest account** as a supplementary service. It is designed to be used for ad-hoc communication with persons not being regular **Flex-users**.
The guest account is an account that can only receive calls or text messages from the owner of the guest account. The guest account is only visible to the owner of the account, and he/she can see when the guest is logged in, and can call or send a text message to the guest. The guest can then answer or reply on received messages.
Any text messages and files will automatically be deleted when a different guest logs into the guest account.

If you are having a personal guest account at your disposal you will have an entry in the address list in the form «**Guest Your name**».

3.9 Passwords

It is up to your organization to set internal requirements to passwords exceeding the minimum for the Flex-service:

- Minimum password length is 3 characters. Recommended length is at least 8 characters.
- There are no requirements to use caps/non-caps characters, numbers or special characters, but it is recommended to use this to secure access to the account.

It is highly recommended that the users change the password already at first time log-in!

It is recommended that the password for the Flex Guest account is NOT changed!
The account cannot be misused in any way, and keeping the password unchanged simplifies the user's administration of the account.
The standard guest account password is printed on your Flex User card.

3.10 PIN-code

As a **Flex-user** you must choose a **PIN-code** for identification purposes when communicating with **Seccom**. The code must be used in connection with temporary blocking the **Flex-account**, or resetting of the password to the activation password. The **PIN-code** is known only to the user and to **Seccom Support**, and consists of a minimum of 4 characters or numbers. This **PIN-code** will have to be given over an unsecured channel in most cases, and it is therefore recommended that sensitive information (like password, payment card PIN-codes etc.) is not used as **PIN-code**.

If you forget the **PIN-code**, your **Flex Main Administrator** can request blocking the account or resetting the password on behalf of the **Flex-user**.

3.11 Flex User card

Each user obtains a **Flex User card**. This is delivered either directly to the user in connection with a user training session, by post to the user or via your **Flex Main Administrator**.

NTS Norway Silentel®

Send a message with "**BLOCK**", "**RESET**" or "**RESET GUEST**" together with your **NTS ID** and **PIN** code by SMS or email to block your account or reset password.

Exchange **username** and **NTS ID** with your contacts and send to **NTS** to connect on **Silentel.**

Tel/SMS: +47 400 51 085 email: support@ntsnorway.com

NTS ID	Flex Guest username	Guest PWD
4700351	g4700514	kjm

Seccom Flex

Send a message with "**BLOCK**", "**RESET**" or "**RESET GUEST**" together with your **Flex ID** and **PIN** code by SMS or email to block your account or reset password.

Exchange **username** and **Flex ID** with your contacts and send to **Seccom** to connect on **Flex.**

Tel/SMS: +47 400 51 085 email: support@seccom.no

Flex ID	Flex Guest username	Guest PWD
4700202	g4700395	msg

Flex User card contains the following information:

- Your personal **Flex ID number**
- Username and password to your personal **Flex guest account** (supplementary service)
- **Seccom Support** telephone number
- **Seccom Support** e-mail address

- Short instructions on how to block the account or reset the password
- **Flex Grid card** (to verify that the correct **Flex server** is connected)

Flex ID number is used together with the **PIN-code** for identification purposes when communicating with **Seccom**.

The card contains **no confidential information** that alone can be misused, but it does contain important practical information to the user. It is therefore recommended that the user always has the card available when using **Silentel**.

3.12 Verification of the Flex-server using the Flex Grid Card

On the back of your **Flex User card** is a 4x4 table that can be used to verify that the correct **Flex** server is connected. The **Silentel** application calculates a value from the server's digital certificate that it is not possible to copy or falsify, and guarantees that the correct communication server is used.

It is not necessary to perform the verification procedure for each login since the application will display a warning if a mismatch between the digital certificates on the user's device and the server.

It is recommended to verify the server **on first login** and later with **regular intervals**.

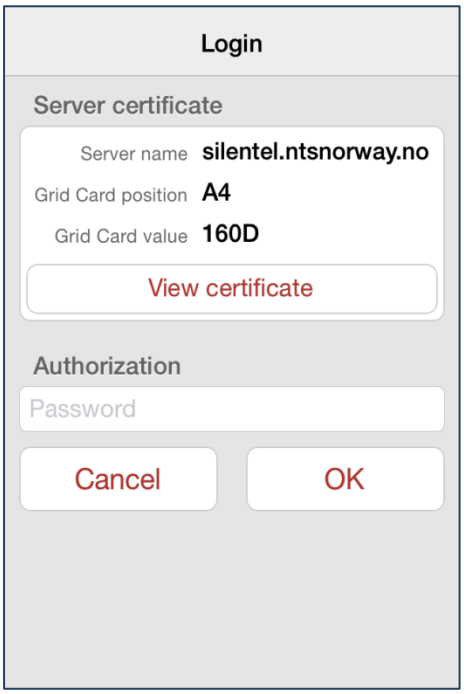
	1	2	3	4
A	4F 13	9A 2C	E4 86	16 0D
B	73 E7	FE 8E	1D D6	66 46
C	34 72	99 3D	E4 EB	E1 21
D	FB 90	D2 D8	45 7B	27 C4

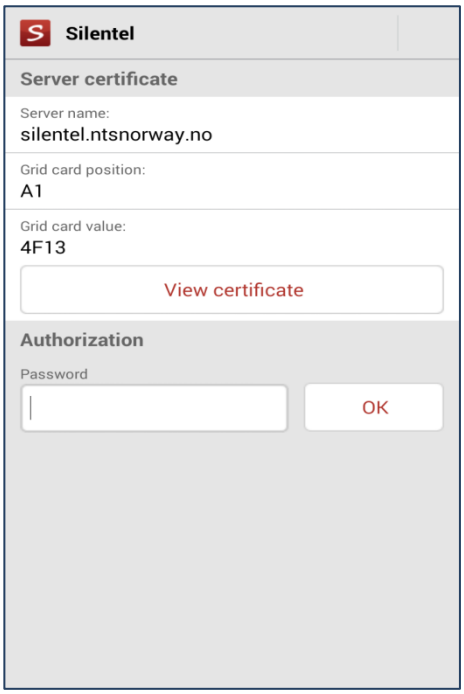
Authority: http://silentel.ntsnorway.no:8080/CAEA-war/Cert/casign.cer
Please report found card to support@ntsnorway.com

	1	2	3	4
A	4F 13	9A 2C	E4 86	16 0D
B	73 E7	FE 8E	1D D6	66 46
C	34 72	99 3D	E4 EB	E1 21
D	FB 90	D2 D8	45 7B	27 C4

Authority: http://silentel.ntsnorway.no:8080/CAEA-war/Cert/casign.cer
Please report found card to support@seccom.no

This can be done in the login window before the password is entered:





The value in the given grid card position must be the same as the application displays.
If these values do not correspond, Silentel cannot be used and this must be reported to Seccom Support immediately!

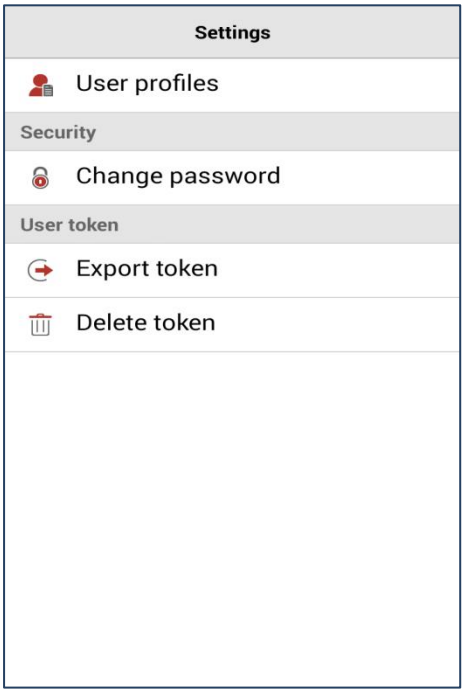
3.13 User token and using multiple mobile devices

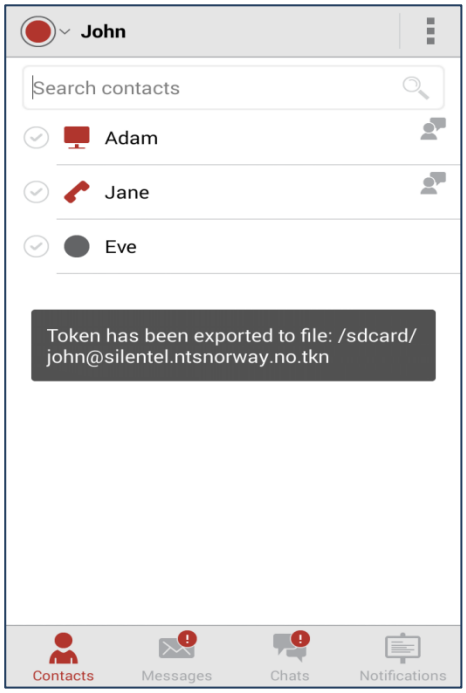
A private encryption key (stored in the so-called **User token**) is used for encrypting text messages, files and mails. This key is stored on the device that is used when logging in the first. If the **User token** is not present on the device used, it will not be possible to access stored messages. If the **User token** is deleted or a new **User token** is generated, all the stored messages on the **Flex** server will be deleted.

In order to use **Silentel** alternately on multiple devices without deleting stored messages, it is necessary to export the **User token** from the **Silentel** application on the original device and import the **User token** on the other devices.

3.14 Export and import of User token – Android and PC

On and Android device, the **User token** can be exported or imported directly in the **Silentel** application by selecting **Menu**, **Settings**, **Export token** / :





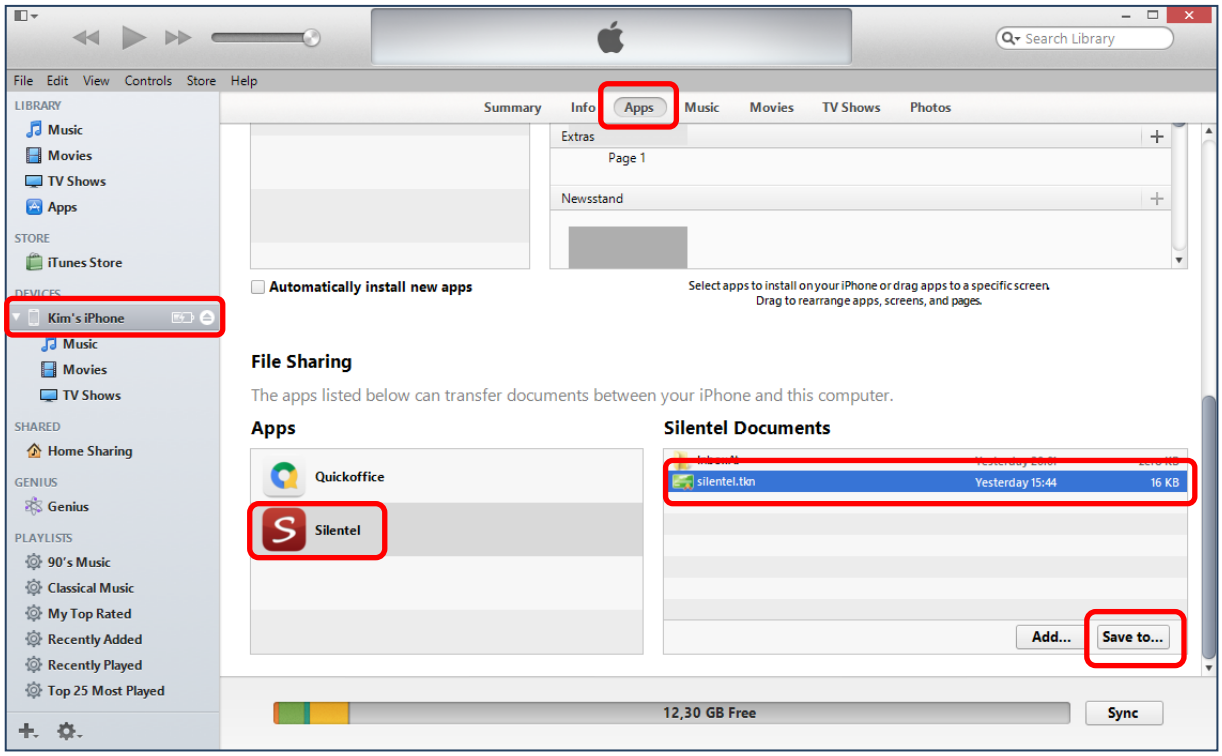
The **User token** is stored as a file that can be transferred to another device or PC and be imported in the **Silentel** application as shown above.

On a PC, the **User token** is exported in a similar way by selecting **Options**, **User token** and clicking **Export token** / **Import token**.

3.15 Export and import of User token – iPhone and iPad

The Apple operating system iOS handles files in a different way than Android and PC, and the program **iTunes** must be used in connection with exporting and importing of User token.

Start **iTunes**, connect the iPhone/iPad and click on the device in **iTunes**. Choose **Apps**, **Silentel** under **File sharing**, **Silentel.tkn** under **Silentel documents** and **Save to** / **Add** to export / import the **User token**.



3.16 Loss of device

Obtaining only the username and password will **NOT** grant access to messages stored on the server since they are always encrypted with the user's private key. This private key is stored in encrypted form on the user's device (in the **User token**), and without this key it is not possible to access any stored content. To access stored messages one must have access to the username, password and the **User token** from the user's device.

If the user is logged in when the device is lost, it will be possible to access stored messages from the lost device until the user logs in from a different device or the account is blocked.

If the device is lost, the fastest and easiest solution is to log in to the user account from a different device, generate a new **User token** and change the password. This will prevent any unauthorized access.

Generating a new **User token** invalidates the original private encryption key, and **all messages and files on the server will be deleted**.
This CANNOT be reversed and deleted messages and files cannot be restored in any way!

3.17 Temporary blocking the Flex account

Send an SMS or e-mail with the text "**BLOCK**" to **Seccom Support** to temporarily block your **Flex** account. The message must also contain the following information:

- Your **Flex ID number**
- Your **PIN-code**

The message to **Seccom Support** can be sent from any telephone number or email account as long as the correct **Flex ID number** and **PIN code** is given. This will not affect messages stored on your **Flex** account.

To reopen your **Flex** account, please send an SMS or e-mail with the text "**UNBLOCK**" to **Seccom Support** together with your **Flex ID number** and **PIN code**.

3.18 Resetting the password

Seccom has no knowledge of the password set by the user after account activation or any possibility to identify the password. **Seccom** will not set a password on behalf of the user to secure that the password is only known to the user himself/herself.
Seccom Support can only reset the password to the original activation password, and the user can then change the password in the **Silentel** application.

To reset the password, send an SMS or e-mail with the text "**RESET**" to **Seccom Support** together with the following information:

- Your **Flex ID number**
- Your **PIN-code**

Seccom will send out the activation password to the e-mail address registered on the user.

PLEASE NOTE:
THE PASSWORD IN USE BEFORE RESETTING IS NEEDED TO ACCESS STORED MESSAGES!
IF THIS ORIGINAL PASSWORD IS FORGOTTEN THERE IS NO POSSIBILITY TO ACCESS THESE!

4 How to secure your Flex account

The **Flex** communication service with the **Silentel** platform offers secure communication on the highest level, and protecting access to your account can be done with a few simple steps:

1. Choose a password with at least 8 characters consisting of upper- and lowercase letters, numbers and special characters
2. Register a **PIN-code** for communication with **Seccom Support**
3. Secure access to your mobile phone with the possibilities that your mobile can offer (unlock passcode/password, finger print scan etc.)
4. Export the **User token** from the **Silentel** application and save it in a safe place so it can be imported on a new device in case of loss/theft of the device. This secures that messages are not lost due to loss of the **User token**. It may be appropriate that **Flex Main Administrator** safeguards this.
5. If possible implement a Mobile Device Management solution that prevents accidental installation of unwanted programs on the device used for Flex to avoid spyware.
6. Do not leave your device unattended at any time when others can access it. If the mobile or tablet must be left outside a meeting room you should use SecBag sealing bags to prevent and detect unauthorized access to the device.
7. It is recommended that the user is logged on to Silentel at all times to increase use of the system.
   It is, however, recommended to log out of the Silentel application in situations where unauthorized access to the device can be expected, e.g. security checks on airports. This will prevent unauthorized access to stored messages.

5 Possible technical problems and solutions

5.1 Problems in connection with logging in

If problems are experienced in connection with logging in to **Silentel**, the following should be checked:

- Is the field „**Server**“ in the log-in window filled in with „**silentel.ntsnorway.no**“ ?
  Please note it should be .no and not .com!
- Is WiFi used for Internet connection?
  If a Firewall is set up to protect the wireless network, the ports that **Silentel** uses for communication with the server are most likely closed.
  In most cases your IT-department can open the ports in question (see chapter 5.4 Firewall settings), but it may take some time and must be handled by your IT-administrator.
  To avoid this problem it is recommended to switch to cellular data (mobile data connection from your mobile operator) to overcome this problem, and get the necessary ports opened when possible.

5.2 Problems with sound delay or echo in voice calls

The implementation of the Android operating system in some models can lead to a noticeable delay in **Silentel** voice calls. This is experienced as the participants “talking at the same time”. This will vary with the type of Internet connection used (mobile data 2/3/4G or WiFi).

If such a delay is experienced it is recommended to try a different Internet connection. If this does not solve the problem, a different device must unfortunately be used.

This type of delay may be cumulative and increase over the duration of the phone call. In such cases a simple solution is to hang up and call again to reset the connection.

Echo can also be experienced on certain Android models and when the Internet connection is poor or unstable. Please consider using a different device if the problem prevails.

Please report any such problems to **Seccom Support** with information about the device used to identify and possibly solve the problem.

5.3 Fast discharging the battery

Normal use of **Silentel** will not affect battery life noticeably, but certain Android models can experience heavy battery drainage.

The only solution to this problem is to use a different device.

Please report any such problems to **Seccom Support** with information about the device used to identify and possibly solve the problem.

5.4 Firewall settings

If **Silentel** is to be used on a computer on a LAN or on a device connected to a WiFi protected by a Firewall, it may be necessary to open certain ports in the Firewall to the **Flex server**. This can easily be checked by trying to log in to **Silentel** and set up a voice call. If this is possible, it will not be necessary to do any changes in the Firewall settings.

If it is not possible to either log in or make calls, the following Firewall ports must be opened for communication with the **Flex** -server:

- **5063 TCP** – SIP Listen port (between the **Silentel** application and the **Flex** server)
- **8080 TCP** –CRL download (Certificate Revocation List from the Certificate Authority) for verification of certificates
- **15060 – 16060 UDP** – RTP ports (for voice communication)
  The entire interval between 15060 and 16060 must be opened, but only towards the **Flex** server's IP-address.

Source IP address: port	**Destination IP address: port**	**Protocol**
any: any	46.226.8.132: 5063	TCP
46.226.8.132: 5063	any: any	TCP
any: any	46.226.8.132: 15060-16060	UDP
46.226.8.132: 15060-16060	any: any	UDP

The **Flex server** has the domain **silentel.ntsnorway.no** with the IP-address **46.226.8.132**. The ports must therefore be opened towards this IP-address.

6 Seccom Support

You can contact **Seccom Support** in the following ways:

- SMS/telephone: +47 400 51 085
- E-mail: support@seccom.no
- Silentel: Seccom Support

Opening hours 08:00-17:00 CET.